



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/081,500	02/22/2002	John Owlett	GB920010095US1	1505

46590 7590 01/24/2006

MYERS BIGEL SIBLEY SAJOVEC P.A.  
PO BOX 37428  
RALEIGH, NC 27627

EXAMINER
----------

LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 01/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 10/081,500	<b>Applicant(s)</b> OWLETT, JOHN	
	<b>Examiner</b> Christian La Forgia	<b>Art Unit</b> 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 09 November 2005.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-14 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. The amendment made of 09 November 2005 has been noted and made of record.
2. Claims 1-14 have been presented for examination.

### ***Response to Arguments***

3. Applicant's arguments filed 09 November 2005 have been fully considered but they are not persuasive.
4. In response to the Applicant's argument that the cited references do not teach adding a spoiler to the challenge, the Examiner disagrees. The Applicant defines a spoiler on page 8 of the specification as "be[ing] added to the challenge as a prefix or a suffix and the authenticating entity extracts the challenge by counting the number of bytes from the beginning or end of the combined spoiler and challenge." Hara discloses adding padding to data and then encrypting the data along with the padding data, because the data is then better suited for encryption (see paragraphs [0083] and [0084]).
5. Hara does provide the missing parts of Andersson, by providing a technique for adding data to the challenge.
6. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the references provide a teaching, suggestion and motivation for combining

Art Unit: 2131

the references. As disclosed in Hara, in particular paragraph [0084], adding padding data makes the data to be encrypted better suited for encryption.

7. In response to the Applicant's argument that the question of motivation to add padding data is based on subjective belief and unknown authority, the Examiner disagrees and contends that adding padding to data has been well known since at least March of 1998. **PKCS #1: RSA Encryption Version 1.5**, by B. Kaliski, discloses the use of adding padding to data to prevent attackers from recovering data by trying all possible encryption blocks, as discussed on page 9. Kaliski also discusses adding padding to data throughout the rest of the technical paper.

8. Therefore, the Examiner reasserts that it would have been obvious to one of ordinary skill in the art at the time the invention was made to add padding data to the challenge in order to make the encryption more secure, by preventing attackers from recovering the data.

9. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

10. See further rejections that follow below.

***Claim Rejections - 35 USC § 103***

11. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

12. Claims 1-5 and 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Application Publication No. 2002/0034301 to Andersson, hereinafter Andersson, in view of U.S. Application Publication No. 2004/0202328 to Hara, hereinafter Hara.

13. As per claims 1, 13, and 14, Andersson discloses a method for authentication of a user by an authenticating entity comprising the steps of:

the authenticating entity sending a challenge to the user (page 3, paragraph [0040], i.e. the authentication server issues a challenge to the user);

the user encrypting the challenge using a private key of an asymmetric key pair (page 3, paragraph [0040], i.e. the authentication token encrypts the challenge with the user's private key);

the user sending a response to the authenticating entity in the form of the encrypted challenge (page 3, paragraph [0040], i.e. the authentication token encrypts the challenge with the user's private key, and returns it to the authentication server).

14. Andersson does not disclose the user adding a spoiler to the challenge and encrypting the combined spoiler and challenge.

15. Hara discloses adding padding to data and encrypting the data and the padding information (Figures 7b, 7c, page 5, paragraphs [083], [0084]).

16. It would have been obvious to one of ordinary skill in the art at the time the invention was made to add padding data to the password and encrypting the password with the padding data, since Hara discloses at page 5, paragraphs [083], [0084] that padding data makes it better suited for encryption, as it is known that padding data to a certain length makes the encryption

Art Unit: 2131

stronger, which is desirable when trying to prevent transmitted password information from being intercepted.

17. Regarding claim 2, Andersson teaches wherein the method includes the authenticating entity decrypting the encrypted combined spoiler and challenge using the public key of the asymmetric key pair and determining if the user has been authenticated (page 3, paragraph [0040], i.e. the returned challenge is then decrypted by the authentication server with the user's public key).

18. Regarding claim 3, Hara teaches wherein the addition of spoiler to the challenge is carried out by applying spoiler function to the challenge (Figures 7b, 7c, page 5, paragraphs [083], [0084]).

19. With regards to claim 4, Hara teaches wherein the form the spoiler function is sent to the authenticating entity (Figures 7b, 7c, page 5, paragraphs [0084], i.e. knowing where the padding is located in order for it to be removed later).

20. Regarding claim 5, Hara discloses wherein the spoiler is added to the challenge as a prefix or a suffix and the authenticating entity extracts the challenge by counting the number of bytes from the beginning or end of the combined spoiler and challenge (page 5, paragraphs [0084]).

21. Regarding claim 11, Andersson teaches wherein the challenge is a bit sequence (page 1 paragraph [0007], i.e. Wireless Application Protocol transmits data in binary sequence).

22. Regarding claim 12, Hara discloses wherein the spoiler is an additional bit sequence (page 5, paragraphs [083], [0084]).

23. Claims 6-8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andersson in view of Hara as applied above, and further in view of U.S. Patent No. 6,072,875 to Tsudik, hereinafter Tsudik.

24. Regarding claim 6, Andersson and Hara do not wherein the method includes the user obtaining a digest of the combined spoiler and challenge before the step of encrypting.

25. Tsudik teaches wherein the method includes the user obtaining a digest of the challenge before the step of encrypting (column 3, line 59 to column 4, line 11).

26. It would have been obvious to one of ordinary skill in the art at the time the invention was made to obtain a digest of the combined spoiler and challenge, since Tsudik states at column 4, lines 12-21 that such a modification would allow for mobile users while minimizing the traceability and possibility of identifying the mobile user.

27. With regards to claim 7, Tsudik discloses wherein the user obtains the digest by applying a hash function to the combined spoiler and challenge (column 3, line 59 to column 4, line 11).

28. With regards to claim 8, Tsudik teaches wherein the user sends details of the spoiler and the method of obtaining the digest to the authenticating entity (column 6, lines 42-63, i.e. home domain authority keeps track of user).

29. Regarding claim 9, Tsudik teaches wherein the user sends details of the algorithm used for encryption to the authenticating entity (column 5, lines 27-48).

30. It would have been obvious to one of ordinary skill in the art at the time the invention was made to send details of the encryption to be used by mobile users, since Tsudik states at column 4, lines 12-21 that such a modification would allow for mobile users while minimizing the traceability and possibility of identifying the mobile user.

31. Concerning claim 10, Tsudik discloses wherein the authenticating entity obtains a digest of the combined spoiler and the original challenge that the authenticating entity sent to the user and compares the digest a digest obtained by decrypting the response from the user (column 3, line 59 to column 4, line 11).

### ***Conclusion***

32. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

33. A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period



Art Unit: 2131

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


34. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792.

The examiner can normally be reached on Monday thru Thursday 7-5.

35. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

36. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia  
Patent Examiner  
Art Unit 2131  
clf

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100